VULNERABILITIES IN FOSCAM IP CAMERAS

F-Secure

Contents

Introduction

The Internet of Things is no longer a futuristic idea – it's upon us. Gartner forecasts that 8.4 billion connected things will be in use worldwide in 2017, and will reach 20.4 billion by 2020. Smart things promise a multitude of cost savings and efficiencies.

But these benefits could potentially be offset by the security risks they pose. F-Secure and companies like us are regularly discovering vulnerabilities in smart devices that have been engineered without regard for security. Insecure IoT devices increase the complexity of the company attack surface. As "things," they are often not regarded as network devices and thus their risk to the rest of the network may be underestimated.

F-Secure's discovery of multiple flaws in two models of Foscam-made IP cameras is another example of a poorly engineered device that offers attackers an easy target. Should an attacker infiltrate the company network and find such a device, they could infect it with malware that would not only fully compromise the device, but also grant free reign inside the network, including access to network systems and resources.

This paper details the vulnerabilities inside the Foscam IP cameras and their impact, and offers mitigation recommendations.

Overview

Foscam-made IP cameras have multiple vulnerabilities that can lead to full device compromise. An unauthenticated attacker can persistently compromise these cameras by employing a number of different methods leading to full loss of confidentiality, integrity and availability, depending on the actions of the attacker.

For example, an attacker can view the video feed, control the camera operation, and upload and download files from the built-in FTP server. They can stop or freeze the video feed, and use the compromised device for further actions such as DDoS or other malicious activity.

If the device is in a corporate local area network, and the attacker gains access to the network, they can compromise the device and infect it with a persistent remote access malware. The malware would then allow the attacker unfettered access to the corporate network and the associated resources.

---

[1] Gartner Press Release, "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016," February 7 2017. http://www.gartner.com/newsroom/id/3598917

Affected devices

Foscam manufactures a number of IP cameras, some of which are white-labeled and sold under various other brand names, one of which is OptiCam. Our consultant investigated two models of Foscam-made cameras: the OptiCam i5 HD device and the Foscam C2.

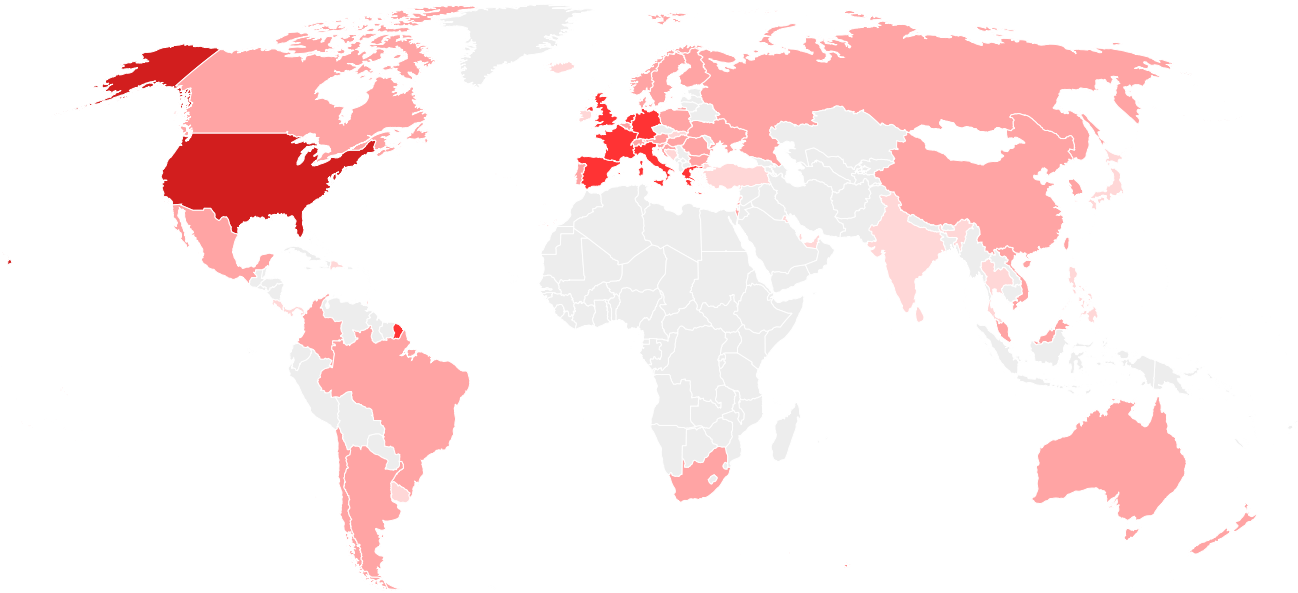
All of the vulnerabilities detailed in this paper have been confirmed to exist within the OptiCam i5. While this device is not listed as an official Foscam product, it is manufactured by Foscam. Many of these vulnerabilities have also been confirmed to exist in the Foscam C2.

While only two models have been investigated, it is likely that many of these vulnerabilities also exist in other models throughout the company's product line, and in other products Foscam manufactures and sells under other brand names. F-Secure knows of at least 14 other brands that market Foscam-made devices:

- Chacon
- Thomson
- 7links
- Opticam
- Netis
- Turbox
- Novodio
- Ambientcam
- Nexxt
- Technaxx
- Qcam
- Ivue
- Ebode
- Sab

The following devices are known to be vulnerable:

Model Name	**System Firmware Version**	**Application Firmware Version**
Opticam i5	1.5.2.11	2.21.1.128
Foscam C2	1.11.1.8	2.72.1.32



Tens of thousands of potentially vulnerable devices are exposed to the internet around the world.

Vulnerabilities

F-Secure has identified 18 different vulnerabilities in the Opticam i5. Many of these have also been found in the Foscam C2. Some of the vulnerabilities are very severe and easily exploited by an attacker. Others require more effort to exploit, but had the more glaring flaws not existed, would be targets in themselves.

The sheer number of vulnerabilities offers an attacker multiple alternatives in compromising the device. Among the discovered vulnerabilities are insecure default credentials and hard-coded credentials, both of which make it trivial for an attacker to gain unauthorized access. Other vulnerabilities allow for remote command injection by an attacker. World-writeable files and directories allow an attacker to modify the code and to gain root privileges. Hidden Telnet functionality allows an attacker to use Telnet to discover additional vulnerabilities in the device and within the surrounding network. In addition, the device's "firewall" doesn't behave as a firewall, and it also discloses information about the validity of credentials.

Some of these flaws can be combined with others to achieve greater degrees of privilege within the device and the local network.Below is a list of each of the 18 vulnerabilities.

INSECURE DEFAULT CREDENTIALS (CWE-255)

Insecure default credentials constitute a widespread problem with smart devices. When the default credentials set by the manufacturer are non-random or empty and when they have not been changed by the user, a remote attacker can gain privileged access to the device. The use of insecure default credentials can lead to the device being infected with malware that co-opts it as part of a DDoS-performing botnet, or can open the device up to other malicious activity.

1. Non-random default credentials for web user interface account

The devices use non-random default credentials of admin:(blank) to access the web user interface. In addition to gaining access to the device, an attacker could upload and download files with the built-in FTP server and can watch the RTSP video feed.

2. FTP server account uses empty password

The user account for the built-in FTP server has an empty password. This makes it easy for an attacker to gain access to the server and download and upload files.

HARD-CODED CREDENTIALS (CWE-798)

Credentials that have been hard-coded by the manufacturer cannot be changed by the user. If the password is discovered and published on the internet (which often happens) attackers can gain access to the device. And as all devices have the same password, malware attacks such as worms can easily spread between devices.

3. FTP server account has a hard-coded password

The built-in FTP user password is hard-coded. This, combined with the fact that the hard-coded password is also empty (#2), means that it is highly likely that malicious actors will gain access to the account.

4. Configuration back-up file is protected by hard-coded credentials

The encrypted Foscam device configuration file contains the admin password, but this file can be exported from the device, and it is protected by hard-coded credentials which cannot be changed by the user. An attacker who has analyzed the device and discovered the hard-coded credentials can, if they manage to obtain the config back-up file, use these credentials to decrypt the file and discover the admin password inside the file.

5. Hidden hard-coded credentials for web user interface

All Foscam models have hidden and hard-coded credentials that allow access to the device regardless of the currently configured users. These credentials enable access to some of the device web user interface functionalities. The functionalities allowed vary depending on the model of the device.

Some models allow controlling the telnetd service and restoring the device to factory settings. These models include at least `Opticam i5'.

HIDDEN FUNCTIONALITY (CWE-912)

6. Hidden Telnet functionality

The devices have hidden Telnet functionality that is not documented anywhere in the specifications. The use of Telnet allows an attacker to more easily find other vulnerabilities in the device, as well as in the local network.

COMMAND INJECTION (CWE-77)

A command injection vulnerability becomes possible when software does not sufficiently validate input from the user. It allows an attacker to insert special characters that let them introduce their own commands into an application, granting them capabilities they would not otherwise have.

7. Remote command injection in User Add

When adding users, the usrName parameter in the CGIProxy.fcgi addAccount functionality ends up in a command line executed by the shell. Since the web interface is running as root, the command is executed as root as well. Valid administrative credentials are needed for exploiting.

8. Remote command injection in /mnt/mtd/boot.sh via ProductConfig.xml

This persistent command injection vulnerability is in /mnt/mtd/boot.sh:

```
eval $(cat $product_config_path | grep 'modelName' | awk -F ">" '{print $2}' | awk -F
"<" '{printf("MODELNAME=\"%s\"",$1);}')
```

The vulnerability can be exploited by using shell meta characters in the modelName in the /mnt/mtd/app/config/ProductConfig.xml file.

The crafted ProductConfig.xml file can be installed to the device by using the configuration restore functionality. Valid administrative credentials are needed to exploit this vulnerability.

9. Unauthenticated Remote Command Injection via Anonymous ONVIF SetDNS

The Foscam camera ONVIF implementation allows anonymous access. An unauthenticated attacker is able to trigger a remote command execution as root via the `devicemgmt' `SetDNS' method. This particular vulnerability is extremely severe because it does not require credentials to exploit, it allows persistence, and it grants access to the rest of the network.

NOTE: Anonymous access only appear to be possible with some camera models and/or firmware versions. Anonymous access appears to work with at least `Opticam i5'.

INCORRECT PERMISSION ASSIGNMENT FOR CRITICAL RESOURCE (CWE-732)

The software gives a security-critical resource a permissions setting that allows the resource to be read or modified by a wider range of users than is intended. The attacker can access sensitive information, modify code to gain privileges, or destroy data.

10. Incorrect permission assignment for startup script: /mnt/mtd/boot.sh

At system start-up the device executes various startup scripts. The chain of execution at boot time is:

```
/sbin/init -> /etc/inittab -> /etc/init.d/rcS -> /etc/init.d/S90init -> /mnt/mtd/
boot.sh
```

The script /mnt/mtd/boot.sh is world writable, enabling any user to access and modify it. An attacker can modify it with their own commands. The file is stored on a flash storage, so any changes to it will be carried over a system reboot. This allows the attacker to maintain a persistent foothold inside the network, as each time the system is powered on, the file executes.

File permissions:

```
-rwxrwxrwx    1 root     root          7547 May  4 21:50 boot.sh
```

If combined with #2 and #6, this vulnerability allows an attacker to fully exploit the FTP user account, use the device as a foothold and access the rest of the local network.

11. Incorrect permission assignment for directory: /mnt/mtd/app

The directory containing the persistent version of the software being run by the Foscam device is world writable, allowing anyone to add or delete files that could alter the functionality of the system. Due to the insecure permissions, any local user can replace the archives to gain root privileges.

```
drwxrwxrwx    9 root     root             0 Jan  1  1970 app
```

The directory itself contains software archives that are extracted to RAM at boot time:

```
-rw-r--r--    1 root     root        597164 Nov 21  2014 www.tar.xz
-rw-r--r--    1 root     root       2472788 Nov 21  2014 zbin.tar.xzn
-rw-r--r--    1 root     root        519320 Nov 21  2014 zlib.tar.xz
-rw-r--r--    1 root     root       1247616 Aug  5  2014 zmodules.tar.xz
```

MISSING AUTHORIZATION (CWE-862)

When a user is accessing a specific resource or performing an action, the software neglects to perform an authorization check. This allows an attacker to access and modify files and perform actions they should not be allowed to.

12. Administrator Credential Disclosure via Anonymous ONVIF GetStreamUri

The Foscam camera ONVIF implementation allows anonymous access. An unauthenticated attacker is able to extract the administrator user name and password via the `media' `GetStreamUri' method.

NOTE: This vulnerability doesn't appear to exist in some camera models or firmware versions. However, it affects at least `Opticam i5'.

13. Unauthenticated Reboot via Anonymous ONVIF SystemReboot

The Foscam camera ONVIF implementation allows anonymous access. An unauthenticated attacker is able to reboot the device by using the `devicemgmt' `SystemReboot' method.

NOTE: Anonymous access only appear to be possible with some camera models and/or firmware versions. Anonymous access appears to work with at least `Opticam i5'.

IMPROPER ACCESS CONTROL (CWE-284)

14. Firewall (CWE-284)

The Foscam cameras feature a firewall that is supposed to restrict access to the device. However, it in fact only protects access to the web user interface (ports 88 and 443). The IP addresses that are firewalled are still able to access other services, such as ONVIF (888), FTP (50021), RTSP (65534) and telnet (23). It is possible to access RTSP at port 88 too, even though the web log in doesn't work.

The firewall is implemented in a manner that discloses information about credential validity. Invalid credentials lead to error -2, while correct credentials behind a firewalled IP address result in error -8. It is thus possible to perform brute force attacks on credentials even when firewalled.

IMPROPER RESTRICTION OF EXCESSIVE AUTHORIZATION ATTEMPTS (CWE-307)

15. Missing restriction of multiple login attempts

The software does not restrict a user from attempting to log in multiple times with incorrect credentials. Therefore, it is possible to perform brute force attacks against the login credentials. The problem applies to at least the web user interface (ports 88, and 443), FTP (port 50021) and RTSP (ports 88 and 65534). It is likely that the same problem is present in all protocols.

UNCONTROLLED RESOURCE CONSUMPTION (CWE-400)

16. Denial of service of the RTSP video feed

This vulnerability allows an attacker to disconnect or freeze the video feed. The Foscam camera RTSP service (RtspServer) has an implementation flaw when processing the `Content-Length' header. Negative numbers are processed incorrectly and lead to either an RtspServer crash due to out of bound memory read or to a busy loop where the single request is processed forever in a tight loop. Since there is a watchdog service that restarts a crashed service, from the attacker's point of view the hang is preferable.

When executed, the attack disconnects or freezes the current video feed and no new connections can be made. The only way for user to recover the video feed is to reboot the device.

NOTE: This vulnerability doesn't appear to exist in some camera models or firmware versions. However, it affects at least `Opticam i5'.

CROSS-SITE SCRIPTING (CWE-79)

17. Unauthenticated Persistent XSS via Anonymous ONVIF SetHostname

The Foscam camera ONVIF implementation allows anonymous access. An unauthenticated attacker is able to trigger a persistent cross-site scripting attack against the users of the web interface.

The XSS payload will trigger when the `Status' / `Device Information' page is displayed.

NOTE: Anonymous access only appear to be possible with some camera models and/or firmware versions. Anonymous access appears to work with at least `Opticam i5'.

STACK-BASED BUFFER OVERFLOW (CWE-121)

18. Buffer overflow in ONVIF SetDNS

A buffer overflow can lead to crashes or to execution of arbitrary code. The Foscam camera ONVIF implementation allows anonymous access. An unauthenticated attacker is able to trigger a remote stack-based buffer overflow via `devicemgmt' `SetDNS' method. When exploited, the service will crash.

```
Program terminated with signal SIGSEGV, Segmentation fault.

#0  0x41414140 in ?? ()
[Current thread is 1 (LWP 1305)]
(gdb) bt
#0  0x41414140 in ?? ()
#1  0x400b3f84 in ?? ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
(gdb) i r
r0             0x0      0
r1             0x0      0
r2             0x2461e4f        38149711
r3             0x0      0
r4             0x41414141       1094795585
r5             0x41414141       1094795585
r6             0x41414141       1094795585
r7             0x41414141       1094795585
r8             0x41414141       1094795585
r9             0x2431ca0        37952672
r10            0x41166d6c       1091988844
r11            0x41166d68       1091988840
r12            0x400ec254       1074709076
sp             0x41166d40       0x41166d40
lr             0x400b3f84       1074478980
pc             0x41414140       0x41414140
```

```
cpsr            0x60000030      1610612784
(gdb)
```

NOTE: It is likely there are number of similar crashes in the firmware.

NOTE: Anonymous access only appear to be possible with some camera models and/or firmware versions. Anonymous access appears to work with at least `Opticam i5'.

Examples of attacks

1. As unauthenticated user

1.1 Add new root user to /etc/passwd, enable telnetd, log in as root

Using the ONVIF protocol which has empty credentials, anyone able to access a specific port can use a command injection to add a new root user for the device and to enable a standard remote login service (Telnet). Then, when logging in through this remote login service, they have admin privileges on the device.

1.2. Enable telnetd remotely, log in as ftpuser1, install persistent payload

This attack takes advantage of vulnerabilities #2, #6 and #10 to allow the attacker persistent remote access to the device. The empty password on the FTP user account can be used to log in. The hidden Telnet functionality can then be activated. After this, the attacker can access the world-writable (non-restricted) file that controls which programs run on boot, and the attacker may add his own to the list. This allows the attacker persistent access, even if the device is rebooted. In fact, the attack requires the device to be rebooted, but there is a way to force a reboot as well.

2. Authenticated user / not yet configured device

2.1. Add new root user to the system, enable telnetd, log in as root

If the device has not been configured into use yet, an attacker may add a root user in a way similar to example 1.1. The vulnerability exploited is somewhat different, and will require a separate fix.

End user mitigation

To protect the device from being found on the internet and exploited by attackers, we recommend users only install the cameras within a dedicated network or VLAN.

As a best practice, users should always change the default password on their devices to a unique and strong set of characters. However, because of the Foscam IP cameras' use of hard-coded credentials, in this case an attacker can bypass unique credentials.

Corporate users should:

- Segment the network heavily based on trust levels.
- Ensure there is a process for acquiring new software and hardware, and follow the process.
- Never assume anything to be secure without evidence.
- Understand the systems. Do risk and threat modelling, investigate the security track record of the vendor and verify the device can be patched if necessary.
- Before any widespread deployments, do security testing beforehand.

Recommendations to vendor

The responsibility for ensuring the security of hardware and software ultimately lies with the vendors of these products.

Our recommendations to Foscam are as follows:

- Make existing fixes available for all models in a coordinated way.
- Always quote input that ends up commands executed by the shell, or use exec() family functions exclusively. Avoid system() calls. Avoid construct where execl is called with "sh -c %s" since this is same as a system() call.
- Avoid eval in shell scripts on untrusted input.
- Remove unsafe input processing (sprintf, strcpy, strcat, memcpy with untrusted length etc).
- Employ a truly random default administrative password and add a sticker at the bottom of the device with the password.
- Disable the user from the passwd file.
- Remove unnecessary hidden functionality such as being able to enable telnetd.
- Remove factory built-in credentials.
- Implement proper iptables firewall.
- Fix world writable file/directory permissions.
- Always perform proper encoding of HTML special characters.
- Disallow anonymous ONVIF.

F-Secure advises vendors to design security within their products from the beginning. Having product security processes in place and investing even modest resources into security is a differentiator from competitors. This can also work to vendors' advantage when regulation enforces secure design practices.

Vendor response

These vulnerabilities and recommendations have been disclosed to the vendor and the vendor has been given several months to respond. To date no fixes have been issued by the vendor.

Because there appear to be no fixes available, we have refrained from publishing exploit code for practical proof-of-concept attacks.